Intel® Processor Serial Number Applications

Improving Security, Manageability, Information Management, and More

White Paper

intel®

CONTENTS

Executive Summary

As the leading supplier of building blocks for distributed computing, Intel constantly strives to develop microprocessors that provide both the performance and the features needed to run today's applications and tomorrow's. The processor serial number, introduced to the Intel® architecture with the Intel® Pentium® III processor, is a key feature that software developers can use to strengthen their applications for the evolving world of Internet- and intranet-based computing.

Processor serial numbers can add value to a wide range of applications in both business and consumer computing:

Security

E-business depends on the assurance that confidential information is accessed by only the appropriate business partners or employees. Applications that take advantage of processor serial numbers can add another element to system identification and thus increase confidence in using the Internet and the Intel architecture as the platform of choice for electronic business. Similarly, processor serial numbers can strengthen the data security for consumer Web sites that want to maintain a section open only to family members or other subcommunities. It can also be used in businesses for adding a level of validation to electronic signature approvals.

Manageability

Information Technology (IT) departments use a variety of methods to track assets, but none are as reliable as the processor serial number. Other tracking numbers such as network card's MAC address or BIOS's GUID could be changed or erased. Designing applications to use this feature can help IT customers reduce total cost of ownership (TCO) and manage their resources more efficiently.

Processor serial numbers can add value to a wide range of applications in both business and consumer computing

Information Management

Companies can turn information into a competitive advantage if they can manage it effectively. Information-related applications can use processor serial numbers to handle tasks ranging from finding multiple copies of a virus-infected document, tracking change information, to delivering customized information to the end user.

By adding support for processor serial numbers into their applications, developers can increase their applications' value to customers and increase the PC's utility as the primary vehicle for electronic business, Web-based commerce, information management, and other tasks of business and home computing. To assist developers in using processor serial numbers, this brochure describes a reference implementation Intel has worked with leading vendors to develop. This reference implementation provides a framework for obtaining and validating a system's processor serial number over a network. Intel is working with several security tool vendors to enable them to provide these technologies to developers.

Introduction: a New Feature Meets Evolving Computing Needs

The rapid emergence of electronic business and the growth of Internet- and intranet-based computing are expanding the role of the personal computer and creating new needs for secure, trusted, manageable PCs and applications. To help meet these needs, the Intel® Pentium® III processor extends Intel's previous system identification mechanism by adding an "ID tag" for the processor—the processor serial number.

The Intel processor serial number creates a software-accessible identity for an individual processor. A 96-bit number accessible through the CPUID instruction, the processor serial number enables applications to identify a processor, and, combined with other qualifiers, a system or user.

This new CPU feature offers numerous opportunities for software applications to make the PC a more effective tool for both business and home computing users. For e-business and other connected computing applications, the processor serial number can help improve system security, manageability, and information management.

Security

Because the CPU is a persistent element of the system, the processor serial number can be used by networks and applications as a proxy for identifying the system. The processor serial number, when combined with other identification methods such as user IDs and passwords, can also be used in multi-factor authentication. Such usage can enhance the security of business e-commerce, as well as the delivery and access to confidential business documents and other sensitive content.

Manageability

Because the CPU is the "brain" of the computer system, the processor serial number is the most consistent, persistent and reliable identifier for use in system asset tracking, fault recovery in multi-processor servers, and loading software and configuring systems over the network. Having a software-accessible processor serial number gives IT departments a new tool to improve manageability and lower the lifetime costs of managing their computer systems.

Information Management

As the flood of information rises and the PC becomes the primary vehicle for processing, storing and accessing information, the management of information poses a greater challenge. The processor serial number provides a non-intrusive identifier that enables information service providers to customize the data and services that are delivered to the end user. The processor serial number also provides a better way to track and protect important or sensitive information, and it can improve applications such as data backup and restore protection, removable storage data protection, managed access to files, and confirmation of document exchange between appropriate users.

The processor serial number also provides a better way to track and protect important or sensitive information.

On the consumer side, the processor serial number can enhance accountability and provide managed access to sensitive information:

Accountability

Processor serial numbers enable Web sites to manage access to Internet communities by enhancing the ability to identify and restrict problem users.

Security

Processor serial numbers provide an additional mechanism by which users can prevent unauthorized access to sensitive information.

This brochure discusses a variety of ways developers can use the processor serial number to add value to their applications, and includes case studies of companies that are already beginning to benefit from using processor serial numbers. This brochure also summarizes a reference implementation Intel has developed with security vendors that provides a basis for network servers to verify a client system's processor serial number. This Processor Serial Number Verification Reference Implementation (RI) gives application developers a head start on taking advantage of the benefits of the Intel processor serial number.

Enhancing Security for E-business

The Internet enables organizations to transcend traditional cumbersome, time-consuming business practices and move to cost-effective, near-real-time transactions with customers, suppliers and business partners. This gives companies new freedom to push and pull information to and from one another, but also increases the need to validate that information reaches only its intended recipients and is secure from unauthorized access. The Intel processor serial number can be invaluable in this regard.

Individuals and businesses can authenticate who is accessing the information on their personal computers and their company network by combining any two or three variables:

- The traditional "something you know" mechanisms such as login names and passwords.
- "Something you have" items such as hardware keys (dongles), smartcards, digital certificates, and digital signatures.
- "Something you are" aspects such as biometric measures.

With the launch of the Intel® Pentium® III processor and its processor serial number technology, the PC now has the equivalent of a cyberspace address or a "something you have" access token that can be used in conjunction with passwords and, as they become economically feasible, biometric readers and smartcards. The processor serial number can be used to help ensure that only the intended platform receives sensitive corporate information. When combined with an individual's other authentication options, the processor serial number can help organizations prevent confidential information from reaching unintended recipients. For example, a travel agency network can validate a system's processor serial number to make sure that sensitive pricing information is pushed only to authorized travel agents' machines. The increased security afforded by processor

serial number identification also helps corporate intranets extend information to employee desktops, offering employees greater real-time access to their 401(k) plans, payroll, and other personal data once their processor serial number is validated.

In business-to-business transactions, corporations can tie the processor serial number to their digital certificates and internal or external certificate authorities. Business partners can then gain access to private information only if they have their corporate certificate and are accessing the data from a validated platform.

The processor serial number also allows businesses to broadcast sensitive video with synchronized presentations by adding another layer of authentication prior to pushing the presentation out to the user.

Businesses can validate a system's processor serial number before pushing or pulling presentations that contain confidential information, including:

- Intellectual property presentations such as engineering drawings.
- Valuable Wall Street market research reports.
- Legal documents such as nondisclosure agreements and sealed court documents.
- Corporate financial information.

With increased assurance that confidential information is accessed by only the appropriate business partners and that their employee information is protected, businesses can feel even greater confidence in using the Internet and the Intel architecture as their platform to conduct electronic business. This is also important for companies with highly sensitive information, because it can add additional protections besides user ID and password. (For more information on how to validate system identity, see *Reference Implementation for System Verification* later in this document.)

With increased assurance that confidential information is accessed by only the appropriate business partners and that their employee information is protected, businesses can feel even greater confidence in using the Internet and the Intel architecture as their platform to conduct electronic business.

iLumin*: Protecting Sensitive Legal Documentation

Filing legal documents is typically an inefficient, paper-intensive process that's ripe for modernization. As part of a Utah State Court electronic filing pilot project, the Salt Lake County District Attorney's Office, located in Salt Lake City, Utah, wanted to move its processes for filing documents in the State Court System to a completely electronic system. The District Attorney's Office needed to be able to pull information from a case management system built on a relational database, create an original document, and share the document and key data contained in it with other individuals, county departments, and agencies. It also needed to make sure unauthorized users couldn't gain access to confidential legal materials.

The District Attorney's Office chose a solution from iLumin Corporation, based in Orem, Utah, that had been developed as part of the Utah State Court's electronic filing pilot project. iLumin's E-filer solution offered a wide range of features, and improves the transfer, exchange, and sharing of important judicial information throughout the court system and through associated state and county entities. The application automatically routes documents for signatures, authenticates digital signatures and collects electronic cash payments.

To provide additional security measures over and above the digital signature technology, iLumin teamed with Intel to add support for the processor serial number. Through iLumin's use of processor serial numbers, parties to a filing transaction can validate the platform that originated vital documents such as sealed criminal information, search warrants, arrest warrants, and other court filings. This provides a higher level of security to maintain the integrity and privacy of important documents-of-commerce, and to foil unwarranted attempts at repudiating authorized legal documents.

The iLumin solution can be applied to any electronic filing process in any industry that involves legally binding documents, electronic distribution, document processing, docket or database integration, document retrieval or storage, digital signatures, digital cash payments, or the need for document transaction security.

"We are very excited to work with Intel to provide additional security capability to meet the needs of our clients through the use of the Pentium® III processor. The Pentium® III processor's functionality is an advance that is greatly needed today. Security and privacy are big issues in the electronic filing market, and our relationship with Intel enables us to meet those needs in a more comprehensive fashion."

— D. Brent Israelsen
CEO and President
iLumin Corporation

CASESTUDY

CASESTUDY

SABRE Group*: Verifying System Identification

The SABRE Group* is a world leader in the electronic distribution of travel related products, services, and information technology solutions for the travel and transportation industry. The SABRE Group's proprietary network offers more than 30,000 travel agencies and numerous corporations access to the availability, booking, and pricing information of more than 400 airlines, 50 car rental companies, 35,000 hotel properties, dozens of railways, tour companies, passenger ferries and cruise lines located throughout the world. So when The SABRE Group explored the possibilities of using the Internet as a means by which its constituents could gain access to their content, the ability to remotely and reliably identify the location of the platforms became paramount. Accurate imposition of taxes and tariffs from around the world requires a precise knowledge of the location of the travel agency that accesses the system.

As a remedy to this requirement, processor serial number technology was able to provide a persistent identifier that augmented and improved upon the previous identification scheme being used, while also preventing illegal access to the network. Andy Abate, Senior Development Director of Applied Technology*, commented on the value that processor serial number was able to create: "The ability to conclusively identify a machine's location and affiliation provides The SABRE Group with the opportunity to tailor and deliver travel content with an extraordinary degree of control. Combining processor serial number with the Internet potentially expands our available distribution channels while providing us with confidence in the validity of the destination."

Improving Manageability, Reducing TCO

In large enterprise environments, IT managers face daily challenges to ensure a well-managed and smooth-running computing infrastructure. The Intel Pentium III processor and its processor serial number give IT departments a new tool to improve manageability and lower the total cost of ownership (TCO) of PCs. With a consistent, persistent and reliable number by which to identify the processor, IT managers can better track a PC throughout its lifetime, configure new systems, improve security and increase efficiency in multiprocessor and clustered environments. By helping IT departments to automate and simplify these tasks, processor serial numbers can assist IT in improving its service levels while reducing one of the most expensive aspects of support: technician labor.

Processor serial number can reduce TCO and improve system management by helping IT staff to:

Reliably Identify and Manage Hardware and Software Assets

In the past, IT departments utilized a variety of methods, including user name, MAC address, and GUID, to identify hardware. However, none of these methods are as consistent and reliable as the processor serial number, which cannot be erased or changed. With a processor serial number, it's easy to identify a specific PC, even if the system changes users, network cards are swapped out, or the system software and BIOS are reloaded. The processor serial number also makes it possible to report more reliably on software asset management, since IT managers can know with a higher level of certainty the software running on each system and the users of software program. Having this information readily available can aid in deploying new capabilities (since IT can easily determine which systems need a hardware upgrade to run new software). It can also assist Help Desk personnel in troubleshooting problems even when a PC's hard-disk is crashed.

Configure and Upgrade PCs

For system configuration and software updates, companies can use the processor serial number as a way of reliably identifying PCs pre-boot, post installation remotely. If support technicians know the processor serial number ahead of time, they can enter the number in the database and pre-program the software to be delivered when the PC is placed on the network. This reduces on-site engineering visits and automates the configuration process, saving time and reducing support expenses. It also helps maintain a consistent software load, which further increases the environment's reliability and the efficiency with which IT can manage it.

Increase Efficiency in a Multiprocessor and Clustering Environment

Today, if one processor fails in a multiprocessor environment, it's difficult to determine which specific processor failed.

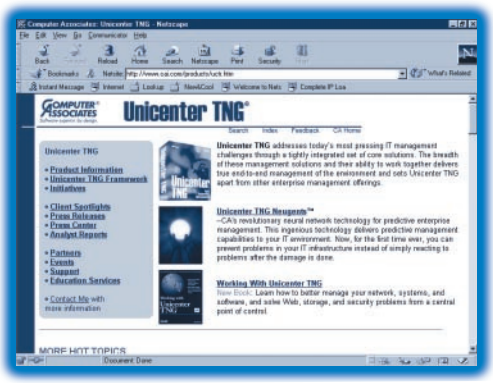
With the Windows NT* operating system, the logical processor can be identified but not mapped to the physical processor. The processor serial number allows IT staff to determine the exact point of failure, so they can route work around the problem processor. This can significantly improve load balancing and fault tolerance and increase the system's availability to the user.

The more critical the PC becomes to a company's strategic mission, the more important it is to manage the computing infrastructure efficiently and cost-effectively and to keep PCs and servers up and running. Processor serial numbers are a valuable tool to help IT departments achieve these goals.

Computer Associates*: Identifying PCs

Computer Associate's Unicenter TNG* is one of the industry's leading enterprise management solution, enabling businesses to optimize their technology infrastructure.

Unicenter TNG's ability to auto-discover the Pentium III processor serial number—the primary key for identifying PCs and Servers—instills a superior level of manageability in tasks requiring unique and indisputable identification, such as asset management and configuration, software distribution, security and more. This powerful solution delivers reliable detection of single or multiprocessor systems. Combining this capability with Unicenter TNG's robust event management offers a comprehensive solution for improved load balancing and fault tolerance in a multiprocessor and clustering environment. Together, Unicenter TNG and the Pentium III processor serial number can save corporations time and money while increasing server availability, by effectively and efficiently managing enterprise-wide assets and configurations.



"We are thrilled to be part of the Intel® processor serial number initiative as the provider of Unicenter TNG—an ideal reference management platform for processor serial number. With Unicenter TNG clients can really capitalize on processor serial numbers to manage assets, configure software, and increase server availability, saving their organizations time and money."

—Yogesh Gupta
Senior Vice President of
Product Strategy
Computer Associates, Inc.

CASESTUDY

Managing Information More Effectively

The Information Challenge

Corporate intranets and the World Wide Web place a wealth of data at every computer user's fingertips, but the sheer volume of information from the Web—news feeds, commercial on-line services, database servers, shared file systems, e-mail, voice mail, fax, etc.—is growing faster than humans can assimilate it. As a result, employees can experience such an information overload that more information sometimes results in less actual knowledge and value.

Information management helps alleviate this overload, and processor serial numbers can play a vital role when creating, copying, storing, retrieving, searching, and sharing information. Processor serial numbers can:

- Make it easier to locate multiple copies of a document.
- Help companies track information and more accurately authenticate information passing through individual machines.
- Support machine-specific user profiles for accessing information.

Locating Copies of a Document

When documents are created and dispersed throughout a company, it can be difficult to know where all the copies have gone. Yet without document tracking, it becomes impossible to find outdated revisions that are still in circulation, locate duplicates of the same media asset, or pull all copies of a document that contain a new virus.

Processor serial numbers can be used as automatic document markers to help companies track documents, even in unstructured environments. This approach is not only highly effective, but also much simpler and more reliable than techniques such as adding name fields and other metadata, which require extra effort by users and are prone to errors. Instead, applications can automatically, non-intrusively, and accurately mark documents with the

Information from the Web—news feeds, commercial on-line services, database servers, shared file systems, e-mail, voice mail, fax, etc.—is growing faster than humans can assimilate it.

processor serial number of the machines used in creating and modifying the documents. This makes it easy to subsequently track documents. For example, if a document is found to have a virus, it becomes relatively straightforward to locate all copies of the document and use the processor serial number markers to identify the machines that need to be disinfected.

Tracking Change Information

Tracking change information is essential in a collaborative environment. With databases or document management systems, processor serial numbers can provide a way of auditing changes: in addition to recording the time stamp and user who made changes, administrators can identify the PC from which the change was made.

Processor serial number applications give users another easy handle for tracking. Rules can be set up to identify which users and on which PCs key modifications can be made; for example, allowing changes in privileges only by the administrator from the administrator's machine.

Processor serial number applications also improve the ability to trace the machine that created, received or approved information. For example, the quality control documentation for an aircraft can exceed 50 Kg of paper, and once it is signed and initialed in many places, it is rarely read unless an investigation is required. The primary reason for keeping paper copies is to authenticate the signatures. By adding the processor serial number of the computer used at each step of the sign-off process, companies can enhance the way they track authenticated signatures. In doing so, they may be able to move a project's quality control and sign-off documentation from a file cabinet full of paper to a single CD.

Improving Access to Confidential or Personalized Information

Businesses often need to provide information to some categories of users and exclude others. For example, a bank may want its customers' complete credit history to be readily available at the loan desk, but not at the teller windows.

With processor serial numbers, access to information can be made machine specific and combined with rules for which systems are allowed to obtain specific types of information. For ease of use, this feature can be implemented without requiring user intervention. This provides a simple way for distributors of valuable information to ensure that their information is delivered only to specific systems.

Processor serial numbers can also help users who want to tie their peripherals to PCs with a specific processor. For example, a Zip* drive with confidential information can be tied to the owner's PC processor serial number, to ensure that the data won't be viewed on a different PC if the drive is stolen.

Individuals can also use their processor serial number to maintain a consistent user profile. For example, users with multiple machines may want to arrange for bills to be sent to their office computer, while digital content goes to their home PC. Or, with time-sensitive information, senders can specify that the information be sent to the first machine to which the user logs on. Users can then maintain a consistent profile, despite using different machines.

BackWeb Technologies*: Customized Information Delivery

BackWeb Technologies is one of the leading providers of push-enabled Internet communications applications that deliver time-critical information to the extended enterprise. Its products enable companies to focus and adapt quickly to changing customer needs and market conditions by improving their ability to rapidly communicate critical information. Its newest offering, the BackWeb Sales Accelerator*, facilitates critical communication throughout the sales chain, which includes the sales force, customers, and partners. More than 250 companies in finance, retail, high-tech, travel and telecommunications are currently using BackWeb's information delivery solutions to impact their bottom lines.

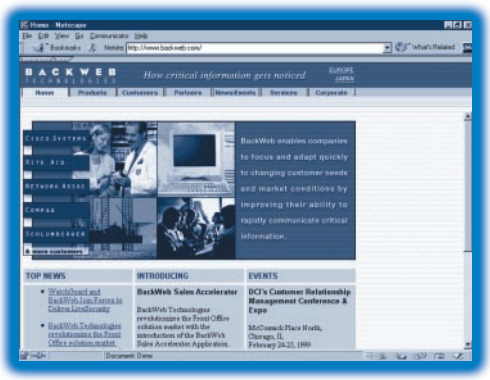
With processor serial number, BackWeb will offer enhanced content targeting and authentication for specific applications using the BackWeb Sales Accelerator. Processor serial number gives the BackWeb Sales Accelerator further granularity for sending the sales team, customers or partners targeted information, such as changes in pricing, new product announcements or competitive data.

"BackWeb's success depends upon its ability to proactively deliver critical information in a timely manner," said Mark Gaydos, BackWeb's Director of Product Management. "Processor serial number, with its improved information access and tracking capabilities, makes BackWeb's technology even more powerful."

BackWeb Technologies

Mark Gaydos

Director of Product Management



CASESTUDY

Accountability and Privacy for Consumers

The uses of the Intel processor serial number are not limited to business computing. In the consumer sphere, this feature can provide an easy-to-use vehicle for creating friendly and accountable Web-based communities, as well as enhancing existing mechanisms that provide access to sensitive information.

Managed Communities

The ubiquitous use of e-mail and the rapid growth of community and chat-based Web sites allow Internet users to reach out and interact with people whom they have never met. Unfortunately, not all individuals who participate in these forums are well-intentioned. Despite the fact that most chat rooms require a user name and password to gain access to the community, a few users, after being denied access for inappropriate behavior, simply assume a new user name, regain access to chat areas and continue their disruptive behavior. This can allow single individuals to destroy the efforts of a group of people and lessen their enjoyment of the on-line experience.

Processor serial numbers offer an effective means of deterring and dealing with this kind of behavior. For special chat rooms which require extra accountability, like chat rooms for minors, Web sites could create responsible chat environments where codes of conduct are enforceable and reliable by requiring that individuals provide their processor serial number (in addition to their username and password) to gain admission to the chat room. If every member of a chat area volunteers his or her processor serial number, the net result is a more secure community that can more effectively deal with potentially threatening behavior. After all, if problem users volunteer to participate in a room that not only encourages but enforces responsible behavior via the use of processor serial numbers, their ability to regain denied access to the chat room can be thwarted, even if they have changed their user name. The Intel® RI (see *Reference Implementation for System Verification*) can provide the framework and support to easily take advantage of this feature.

The ubiquitous use of e-mail and the rapid growth of community and chat-based Web sites allow Internet users to reach out and interact with people whom they have never met.

Talkcity.com*: Creating More Accountable Web Communities

Talkcity.com* is one of the Internet's leading community Web sites, offering a wide selection of theme-oriented chat rooms for its millions of members. One of its most popular areas is the "KidzKorner" section, which features games and topical chats for children ages 6–12.

Keeping the KidzKorner a safe and pleasant interactive community is a high priority at Talk City. The processor serial number offers an effective and user-friendly solution to the problem of inappropriate behavior. By requiring members to submit the processor serial number of their Pentium III processor-based PCs in addition to their user name and password, Talk City can create a more secure community that denies access to individuals who have a record of violating Talk City's behavioral rules.

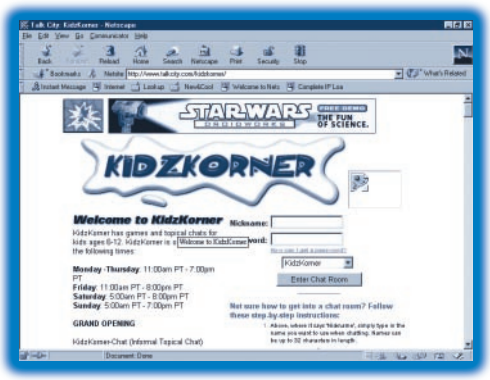
This new capability empowers Talk City to create the kind of communities that parents and children can enjoy time and time again without being disrupted by inappropriate behavior.

"Accountability furnishes the component that's been missing from the effort to bring civilization to the Internet."

—Jenna Woodul
Vice President of Communities
Talk City Inc.

Managed Access

Another usage model that Internet users have quickly adopted is the ability to post information to the World Wide Web itself. A number of companies have been founded to provide this service, with the end result that every Internet user can have his or her own "destination" for friends, family members, and strangers to visit. These destinations in most instances require some form of administrative control to grant both access and editing privileges to the content itself, with user name and password serving as the primary means of identifying the individual requesting privileges.



Talk City Inc.
Jenna Woodul
Vice President of Communities

Ancestry.com
Curt Allen
CEO and President

The need for more robust identification measures is directly proportional to the sensitivity and importance of the posted data. Individuals who are particularly concerned about who can gain access to their posted information and what they might do with it can require that visitors submit their PC's processor serial number in addition to their user name and password. This added level of identification can provide an additional measure of security to users who post sensitive information.

By using the processor serial number, Web sites can strengthen the identification mechanism they currently deploy. Once again, the Intel-developed RI can be used as the vehicle to reliably and consistently retrieve a customer's processor serial number. The RI can also be used to help seamlessly integrate the use of processor serial numbers into a Web site's user or system identification scheme.

Ancestry.com* and MyFamily.com*: Keeping Private Information Private

Two popular Web sites, Ancestry.com* and MyFamily.com* are early adapters in taking advantage of processor serial numbers.

Ancestry.com has established itself as a top subscription service for Web-based genealogical and family history hosting. MyFamily.com offers a unique service to families and other close-knit groups with a free, private place to share and distribute family information on the Web.

Ancestry.com users want secure access to subscription services. Users of MyFamily.com are clear that no information is more sensitive and private than that which involves their family. This is why, when Curt Allen, CEO and President of Ancestry.com, was presented with the processor serial number as an incremental identification mechanism, he was quick to recognize the value it could provide to his customers.

"Intel's innovations have enabled us to expand our company's offering, and thereby expand our customer base. Using the processor serial number, customers of both our sites will gain unprecedented protection of their personal accounts and private family information."

—Curt Allen
CEO and President
Ancestry.com

Reference Implementation for System Verification

Overview

The Processor Serial Number Verification Reference Implementation (RI) offers a framework that Intel has developed with industry security tool vendors to provide a basis for network servers to reliably identify a client system's processor serial number over an open network like the Internet.

The RI provides a protected way to extract the processor serial number from a client system while addressing important issues such as security of data and delays in network transmission.

Security Measures

The RI's software agents are downloaded over an open network, so they are exposed to attacks by hackers. To protect against attacks, these software agents are designed using special tamper-resistant techniques and are appropriately called Tamper Resistant Software (TRS) agents. The TRS agents automatically detect and protect against potential attacks. These agents are available from different security tool vendors. A common set of API functions has been defined and made available to these vendors so that developers can easily use agents from a number of vendors interchangeably.

To provide safety against impostors, the framework adopts a protocol whereby the authentication or verification of the client happens on the server. Agents are used once for a short time and then are discarded, thus enhancing protection.

Privacy Protection

Authentication mechanisms play an important role in Web-based applications. However, some users or businesses may not honor a consumer's right to privacy, and gather personal information about the consumer without consent. Intel has taken several measures, not only in designing the processor serial number, but also in providing the utility tools, to address consumers' privacy concerns. For example, the processor serial number is disabled and enabled by using a processor serial number control utility. Once disabled, the processor must be reset to re-enable the feature, to deter software applications attempting to surreptitiously enable it once it is off.

Intel has taken several measures, not only in designing the processor serial number, but also in providing the utility tools, to address consumers' privacy concerns.

Several RI features work to enhance the protection of a user's data:

- Software agents that gather the processor serial number are packaged in a digital container (a Cabinet file for Internet Explorer*, and a Jar file for Netscape Navigator*) that is then digitally signed by the provider and delivered to the client system. When the Web browser sees the container, it prompts the user to grant access rights to the software, ensuring that the processor serial number cannot be collected without the user's consent.
- The processor serial number, once read, is transformed into another unique identifier by hashing it with a service ID before it is stored on the Web server and used for authentication.
- The service ID is unique to each service provider. This precludes different Web sites from correlating user profiles.
- The hashing algorithm is a one-way, collision-free algorithm, which means one cannot infer the processor serial number given the hashed value and the service ID. Intel also recommends that service providers make their privacy policies available to the consumer.

Performance Considerations

Another important attribute of the RI design is the short download time for the agents. If the size of the software agents is large, the user might have to wait for a long time before getting access. To reduce download times, agents used in the RI are limited to about 35 Kbytes. However, the quality of protection is proportional to the size of agents; the larger the size, the better the protection provided. A balance was reached with a small agent that can protect against attacks for a sufficient time. Protection is augmented by dynamically renewing the agents and by using a time-out mechanism on the server.

RI Architecture

The RI framework consists of a client module, a server module, and a protocol for communication between them:

- The client module consists of "trusted" Java* applets and native code DLLs

(agents). The Java applets and native code agents are packaged together in digital containers (Cabinet files or Jar files) that are digitally signed and down–loaded to the client system. For a pre-existing client application, the native agents can be pulled by the client application instead of being delivered by the server in a Cabinet or Jar file.

- The server module consists of a Web interface that provides access to the Web site, a verification program that controls access to the Web site based on client authentication, and a back-end database system for storing user information such as name, password, and a hashed identifier.

Client Module

The RI has two types of client modules:

- A non-armored module for client registration.
- A TRS armored module for client verification.

The digitally signed containers, when downloaded, prompt the user for permission before execution. If the user grants permission, the agent is invoked through a Java applet. The agent checks for the presence of the processor serial number, and the applet takes the appropriate action based on the agent invoked.

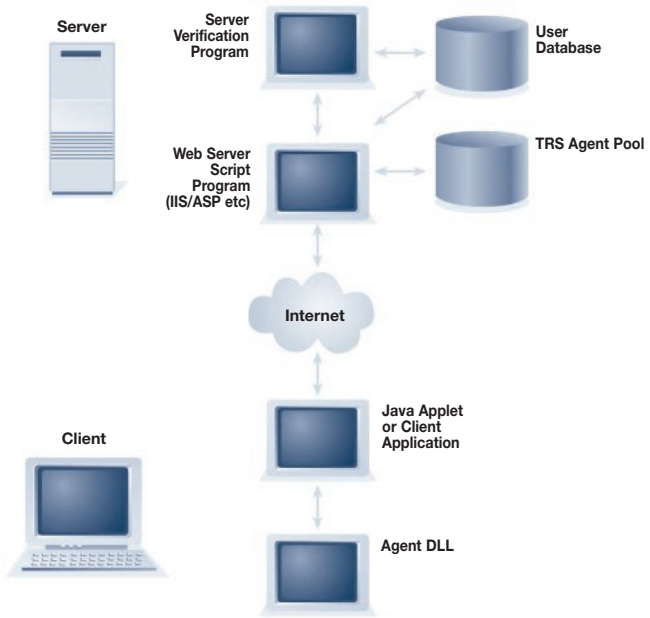


Figure 1: Overview of the RI Application Architecture

Registration Agent

If the client system has the processor serial number feature, the registration agent computes a hash of the processor serial number and service id, and the applet dynamically navigates to a Web page that proceeds with user authentication. If the client system does not have the processor serial number feature, the applet navigates to a different Web page and the user may not gain access to services or protected content.

Verification Agent

Once the client system is identified as having a processor serial number and the user registration process is complete, the armored verification is used for authentication. The server now downloads a different, randomly selected container to the client system. The verification agent hashes the processor serial number and a constant string (the same as the one used for registration). The resulting value is again hashed with additional secret values embedded within the verification agent. This results in an authentication code, which is sent back to the Web server for verification.

Compatibility

Client modules are functional on Microsoft Windows* platforms (Windows NT, Windows 98 and Windows 95). The RI supports the Microsoft Internet Explorer 4.0*, Netscape Navigator 4.x* and AOL* browsers. Both uniprocessor and multiprocessor client systems are supported. For multiprocessor systems, the processor serial number is gathered consistently from the same processor that is selected from the set of available processors.

Server Module

The Web server manages client sessions and authenticates the client system in addition to providing access to the Web site. The Web server also permanently stores the registration code with the user name and password in a back-end database, if one is available.

Managing the Client Session

When a user first logs on to the Web server, the server asks for a user ID and password and then downloads a registration module to the client system. The server stores the returned registration code along with the user's name and password. The server then sends a randomly selected verification

agent to the client, which in turn returns an authentication code to the server. As a measure of extra protection, the server times out during these sessions if it does not receive a response from the client within a pre-determined time interval.

Authenticating the Client

After the server receives a valid authentication code from the client, it first temporarily stores the returned value. Then the server calculates the same hash value that the verification agent computed on the client system. If two match, the client system is authenticated and the user can access content or obtain the requested service.

Commercial Security Tool Products: Rainbow Technologies and Intel's Renewable Security Services Group are currently offering the Tamper Resistant Software agents needed for a protected read of processor serial number. Both vendors have a license for the full RI and plan to offer commercial framework products. To ensure a wide range of product choices to developers, Intel is also working with additional vendors to offer commercial products.

Summary

The Intel Pentium III processor serial number is a software-accessible hardware feature that can be useful for authentication or identification, if retrieved in an appropriately protected manner. The Intel® RI provides a framework for reliably reading the processor serial number from a computer system. The RI can be integrated by Web sites into an existing framework to augment authentication procedures. Intel has licensed this reference implementation to different security vendors. For further information about the commercial security tool products, contact your Intel representative or visit

http://developer.intel.com/drg/pentiumiii/psnum/index.htm.

Conclusion: Delivering Added Value

Intel Pentium III and Pentium III Xeon™ processors are designed and optimized to provide a powerful engine for electronic business and connected computing. The processor serial number is one of many features that makes these processors an ideal foundation for next-generation computing at work and in the home. By designing their applications to take advantage of the processor serial number, developers can increase their applications' value to users and helps their customers create a high-performance, cost-effective computing environment that provides the security, manageability, information management, accountability, and privacy to fully exploit the promise of Internet and intranet technologies.

For more information about incorporating processor serial number support into your applications, contact your Intel account representative or look on the World Wide Web at **http://developer.intel.com/drg/pentiumiii/psnum/index.htm.**

UNITED STATES AND CANADA
Intel Corporation
Robert Noyce Bldg.
2200 Mission College Blvd.
P.O. Box 58119
Santa Clara, CA 95052-8119
USA

Phone: (800) 628-8686

EUROPE
Intel Corporation (UK) Ltd.
Pipers Way
Swindon
Wiltshire SN3 1RJ
UK

Phone:

England	(44) 1793 403 000
Germany	(49) 89 99143 0
France	(33) 1 4571 7171
Italy	(39) 2 575 441
Israel	(972) 2 589 7111
Netherlands	(31) 10 286 6111
Sweden	(46) 8 705 5600

ASIA-PACIFIC
Intel Semiconductor Ltd.
32/F Two Pacific Place
88 Queensway, Central
Hong Kong, SAR

Phone: (852) 2844 4555

JAPAN
Intel Kabushiki Kaisha
P.O. Box 115 Tskuba-gakuen
5-6 Tokodai, Tskubua-shi
Ibaraki-ken 305
Japan

Phone: (81) 298 47 8522

SOUTH AMERICA
Intel Semicondutores do Brazil
Rue Florida, 1703-2 and CJ22
CEP 04565-001 Sao Paulo-SP
Brazil

Phone: (55) 11 5505 2296

Call 1-800-548-4725 to order more copies of this white paper.
Order Number: 245105-001